we have told them that we highly recommend they change RI key at least once a week. / auto down of new key? 1024 RSA key. changing to 2048 in next version.

TRUSTED INFORMATION SYSTEMS, INC.

Building a World of Trust℠

we are giving push exportability of our product, so we are giving them new markets.

U companies we're in negotiations w/ lots of them. we're not interested in providing the service.

FOR IMMEDIATE RELEASE
January 28, 1997

CONTACT: Alla Ziselson
(202) 452-9467
alla_ziselson@oar-wash.com

Includes patent licenses for their own implementation

TWO COMPANIES SET TO OFFER KEY RECOVERY SERVICES USING TECHNOLOGY FROM TIS

Still need to license BSAFE.

TIS' New Key Recovery Center™ Product Shown at RSA

$30,000 to buy toolkit. + 1% of price of crypto product, 5% for multi-user.

RSA DATA SECURITY CONFERENCE, SAN FRANCISCO, CA -- Two firms have announced their intent to offer third-party key recovery services using the Key Recovery Center developed by Trusted Information Systems, Inc. (NASDAQ: TISX) in conjunction with its RecoverKey™ technology. SourceKey and Data Securities International (DSI) have applied for approval to operate Key Recovery Centers to support exported encryption products. (U.S. Department of Commerce approval is required for export of any product incorporating strong encryption.) In addition, TIS also announced today that it is in negotiations with the National Computing Centre, Ltd. of the U.K. and Philips Crypto BV of the Netherlands to license the first non-U.S.-based Key Recovery Centers for third party use.

SourceFile

escrow company.

Key Recovery Centers -- whether privately operated by firms on behalf of their employees or operated by third parties -- are an important element in the user-controlled key recovery approach that TIS pioneered. Key Recovery Centers can, upon an authenticated request, unlock (decrypt) a "spare key" that is generated at the time a given message or file is encrypted. Only the Key Recovery Center is capable of performing this function -- and only if specifically requested, since it does not store or maintain users' keys or data. The "spare key" stays with the message or file until or unless needed.

- more -

3060 Washington Road (Rt. 97), Glenwood, Maryland 21738
(301) 854-6889 • www.tis.com • (301) 854-5363 (F)

"We welcome these new partners who are offering key recovery services," said Stephen T. Walker, President of TIS. "Having Key Recovery Centers in place, and in the hands of the private sector, represents a monumental step forward for global electronic commerce. The infrastructure is coming into being, and we couldn't be more delighted."

Tom Morehouse, President of SourceKey, commented on today's announcement. "We are the first company to be approved by the U.S. Government to be a Key Recovery Center for exported cryptographic products. As an operator of a TIS Key Recovery Center, we are currently the only trusted third party serving customers in this capacity. We look forward to offering key recovery services to more customers as TIS technology becomes an encryption standard."

Adele Revella, Senior Vice President of DSI remarked that "with fifteen years experience protecting source code assets, DSI understands that companies are concerned about trusting a third party with secret information. Yet our customers recognize that it is far safer to work with a trusted partner than to hope nothing goes wrong with their business arrangements. Now companies that want to recognize the full potential of strong cryptography have a similar opportunity to benefit from such a partnership. DSI is pleased that the TIS technology will permit us to focus our experience and reputation on supporting the worldwide expansion of strong cryptography."

TIS also announced availability of its new full-featured Key Recovery Center product that provides user registration and encryption key recovery services. The Key Recovery Center is designed to work with any encryption product incorporating TIS' patented RecoverKey technology. Available now for select customers, the product will be generally available by the end of the first quarter, 1997.

###

About Trusted Information Systems, Inc.

Trusted Information Systems, Inc., is a leading provider of comprehensive security solutions for protection of computer networks, including global Internet-based systems, internal networks, and individual workstations and laptops. The Company develops, markets, licenses, and supports the Gauntlet® family of firewall products and other network security products as well as TIS' patented RecoverKey™ technology, which is the first and only key recovery system to meet US government requirements for export. In addition to providing leading edge information security products, TIS performs an array of services in the areas of cryptography, security consulting, training, and advanced research and engineering for commercial and government customers. The TIS homepage on the World Wide Web is www.tis.com. For more information, contact Bill Thompson, VP Business Development, (512) 263-5936, thompson@tis.com

About SourceKey

SourceKey, a wholly-owned subsidiary of FileSafe Corporation headquartered in Oakland CA, with offices in Atlanta, GA and McLean, VA, was the first organization approved as a Key Recovery Agent to facilitate export of strong encryption products. FileSafe is a world leader in the storage and security of sensitive information for businesses, health care institutions, and governmental agencies, and its SourceFile subsidiary provides software escrow services to the information technology community. For more information, contact Tom Morehouse, President, (510) 832-4300, x127, tommore@ix.netcom.com

About Data Securities International, Inc.

Data Securities International, Inc. (DSI), headquartered in San Francisco, California, is the leading provider of software escrow services in the world, protecting nearly 10,000 licenses in thirty countries. DSI customers include more than 50% of US Fortune 500 companies, and 2,000 of the largest technology companies worldwide. For more information, contact Adele Revella, Senior Vice President, 602-596-2481, arevella@dsiescrow.com

For domestic version, it does it when you want it to
for int'l problem, it does it whether you want it to or not.

TRUSTED INFORMATION SYSTEMS, INC.

Building a World of Trust℠

This is not giving the govt what they wanted initially - they wanted domestic control through key recovery. + they won't get it through this

FOR IMMEDIATE RELEASE
January 28, 1997

CONTACT: Alla Ziselson
(202) 452-9467
alla_ziselson@oar-wash.com

NEW CRYPTO ENGINES FROM TRUSTED INFORMATION SYSTEMS ALLOW EASY INTERNATIONAL USE OF STRONG ENCRYPTION

RSA DATA SECURITY CONFERENCE, SAN FRANCISCO, CA -- Trusted Information Systems, Inc. (NASDAQ: TISX) today announced plans to release its new RecoverKey CSP™ and RecoverKey-International CSP™ Cryptographic Service Provider products. The RecoverKey-International CSP will allow Windows® 95 and Windows NT® users to secure their information by calling on the strongest crypto engine that has ever been made available worldwide.

[redacted] The key recovery center's key must be signed. master key is hardcoded in the code.

The new products work with the Microsoft Windows operating systems to allow the use of strong cryptography across applications, much like Windows' Print Manager allows the use of the same printer for different programs. With CSPs, any application that calls for the use of encryption can encrypt data using algorithms such as DES, Triple-DES, or 128-bit RC2 or RC4. The CSPs also allow key recovery, using TIS' patented RecoverKey™ technology.

"This product will allow Windows users to use encryption as easily as they use a mouse," said Executive Vice President and General Manager of Cryptographic Products Homayoon Tajalli. "The combination of ease of use, proven exportability, and the ability to employ both very strong encryption and, at the user's discretion, key recovery make this a vital advance for both businesses and personal users."

- more -

The RecoverKey-International CSP meets U.S. export requirements, allowing it to be distributed globally, due to its automatic use of the key recovery function. The domestic version of the CSP, available in the U.S. and Canada, provides key recovery as an option, requiring its use only when communicating with a RecoverKey-International CSP. Having domestic and international versions that can communicate with each other is a unique and important capability.

"Previously, if developers wanted to use encryption in their products, they had to consider writing two different versions, dealing with changing export regulations, and so on, and that may have held them back," said Tajalli. "Now, they can write one version of the program and sell it worldwide, knowing that the CSP will handle the encryption legally and safely."

Microsoft recently announced the domestic availability of its enhanced base CSP, which provides the same encrypting strength as TIS' RecoverKey CSP. This CSP, as well as other Microsoft-compatible CSPs, will be fully interoperable with TIS' domestic RecoverKey CSP when key recovery is not enabled.

TIS anticipates the cost of its CSPs, which will begin shipping this quarter, will be less than $100.

###

About Trusted Information Systems, Inc.

Trusted Information Systems, Inc., is a leading provider of comprehensive security solutions for protection of computer networks, including global Internet-based systems, internal networks, and individual workstations and laptops. The Company develops, markets, licenses, and supports the Gauntlet® family of firewall products and other network security products as well as TIS' patented RecoverKey™ technology, which is the first and only key recovery system to meet US government requirements for export. In addition to providing leading edge information security products, TIS performs an array of services in the areas of cryptography, security consulting, training, and advanced research and engineering for commercial and government customers. The TIS homepage on the World Wide Web is www.tis.com.

TRUSTED INFORMATION SYSTEMS, INC.

Building a World of Trust℠

FOR IMMEDIATE RELEASE
January 28, 1997

CONTACT: Alla Ziselson
(202) 452-9467
alla_ziselson@oar-wash.com

TIS ANNOUNCES 6 NEW RECOVERKEY™ PARTNERS

Encryption Market Leaders Entrust Technologies, McAfee, PC Guardian, Philips Crypto BV, Rainbow Technologies, and Secure Computing (Canada) International Join List of Key Recovery Technology Adopters

RSA DATA SECURITY CONFERENCE, SAN FRANCISCO, CA -- Trusted Information Systems, Inc. (NASDAQ: TISX) announced today that the list of companies who have signed letters of intent or otherwise endorsed its RecoverKey™ technology is continuing to grow rapidly. Among the companies now preparing to enable the global use of strong encryption through the use of RecoverKey are: Entrust Technologies, McAfee, PC Guardian, Philips Crypto BV, Rainbow Technologies and Secure Computing (Canada) International (SCI). IBM, Atalla (a Tandem subsidiary) and Hewlett-Packard have previously released related announcements regarding RecoverKey.

"We see this interest as a clear indication that TIS' concept of user-controlled session key recovery is becoming a de facto standard" said Stephen T. Walker, President and CEO of TIS. "The fact that users never give up their private keys is firmly established, and the benefits to users of RecoverKey are now becoming apparent."

RecoverKey allows the secure recovery of the keys needed to decode encrypted data in the event that encryption keys are lost, damaged or unavailable. It creates a separately encrypted backup key that stays with the message or file until needed. The individual "spare key" for an encrypted file can be decrypted, or "recovered" by a selected private sector key recovery center in the event emergency key recovery is necessary.

- more -

The new partners may license the RecoverKey Toolkit so that they can incorporate RecoverKey and/or RecoverKey-International™ into their respective products. RecoverKey-International has already enabled the export of strong encryption products. RecoverKey and RecoverKey-International technology can accommodate any encryption algorithm, and any key length.

Planned product implementations may include the following:

Entrust™ is a unique security solution with fast software-based encryption and digital signature services. Entrust provides automated key lifecycle management features including key backup and recovery and is scalable to any size network. A high-level API allows easy integration into applications and provides a common security architecture across all applications.

McAfee will update its award winning NetCrypto™ network encryption product to allow for key recovery services. The ability to use stronger encryption routines with longer key lengths internationally in regions subject to various export/import controls is critical for success. NetCrypto relies on both the strength of the encryption service plus dynamic key generation for each TCP/IP session between systems running it.

PC Guardian produces software encryption security products that protect data, and is currently planning a key recovery system for PCG's new product, "Encryption Plus™ E-mail". Encryption Plus E-mail is a centrally administered and installed software product that enables Winsock-based E-mail products to send and receive encrypted E-mail without any user intervention or training.

Rainbow Technologies (NASDAQ: RNBO) Internet Security Group (ISG) plans to deliver CryptoSwift™ products providing extremely high performance public key encryption capabilities which are robustly bound to the key recovery process, and are interoperable and compliant with Trusted Information Systems' technology.

- more -

Secure Computing (Canada) International, Inc. (SCI) Cryptoki™ products include cost-effective security tokens, plug-in cryptographic subsystems (APIs and libraries) and off-the-shelf cryptographic solutions. SCI's patented technology includes the Session Key Data Security System -- file and transparent disk encryption to protect confidentiality for information stored on hard drives and floppies and to encrypt individual file content on local and network drives. The Cryptoki Developers Toolkit provides software libraries and test software for integrating tokens in third party applications.

Data on the Philips Crypto (BV) implementation was not available. For more information, contact the company representatives listed below.

RecoverKey Partner Contacts:

Shauna White
Entrust Technologies
shaunaw@entrust.com
613-763-9244

Valerie Christopherson
Rainbow Technologies, Inc.
(714) 374-3530
vchristopherson@msn.com

Tom Clare
McAfee
tom_clare@cc.mcafee.com
408-653-3118

Bob Koblovsky
Secure Computing International
(416) 362-0063
bob@secured.com

Diane Balmer-Martin
PC Guardian
(415) 459-0190
dbalmermartin@pcguardianmail.com

Bill Thompson
Trusted Information Systems
(512) 263-3110
thompson@tis.com

Henk Algra
Philips Crypto (BV)
algraH@crypto.philips.com

###

About Trusted Information Systems

Trusted Information Systems, Inc., is a leading provider of comprehensive security solutions for protection of computer networks, including global Internet-based systems, internal networks, and individual workstations and laptops. The Company develops, markets, licenses, and supports the Gauntlet® family of firewall products and other network security products as well as TIS' patented RecoverKey™ technology, which is the first and only key recovery system to meet US government requirements for export. In addition to providing leading edge information security products, TIS performs an array of services in the areas of cryptography, security consulting, training, and advanced research and engineering for commercial and government customers. The TIS home page on the World Wide Web is at www.tis.com.

TRUSTED INFORMATION SYSTEMS, INC.

Building a World of Trust℠

FOR IMMEDIATE RELEASE
January 23, 1997

CONTACT: Cabe Franklin
Trusted Information Systems
202-452-9504
cabe_franklin@oar-wash.com
or
Tim Blair
IBM Corporation
914-766-1353
tblair@us.ibm.com

TRUSTED INFORMATION SYSTEMS AND IBM ANNOUNCE PATENT AND SOFTWARE LICENSE AGREEMENT

(Glenwood, Maryland) -- Trusted Information Systems (NASDAQ: TISX) and IBM (NYSE: IBM) today announced a patent and software license agreement which will accelerate the use of strong encryption, better enabling the growth of secure e-business worldwide.

Under the terms of the agreement, IBM acquires the right to license and distribute TIS's patented RecoverKey™ technology within the IBM SecureWay Key Management Framework, as well as in IBM products which will need key recovery technology.

"The synergy between two market leaders offers customers the broadest scope of security solutions," said Kathy Kincaid, Director of I/T Security Programs at IBM. "By entering into this agreement, we are accelerating the growth of widespread encryption, giving our customers what they need -- a more secure environment to conduct global e-business."

Steve Walker, President and CEO of TIS, concurred. "This agreement shows that RecoverKey can be what we've always hoped it would: a tool to facilitate the widespread availability of strong encryption around the world. Through this licensing agreement, both companies have proven their commitment to helping bring about an international electronic economy."

Under the terms of the agreement, IBM can incorporate RecoverKey into its suite of software products. IBM may also create a software toolkit using RecoverKey to be licensed by other vendors for their own cryptographic applications. IBM is also licensing TIS's Key Recovery Center software, which provides recovery operations in the event an encryption key is lost or damaged.

-- more --

RecoverKey is the first key recovery technology to work within IBM's SecureWay Key Management Framework, announced last month at Internet World. The SecureWay approach promotes the coexistence and interoperability of various key management systems and key recovery technologies, enabling more rapid deployment of key recovery to customers. TIS commended this approach today.

"RecoverKey was created to meet the needs of an evolving marketplace." said TIS Executive Vice President and General Manager of Cryptographic Products Homayoon Tajalli. "We designed RecoverKey to function with both current and future applications and standards, and it will continue to evolve as the market matures. Being a part of the SecureWay Key Management Framework helps us achieve our goal."

Note: Comments regarding this agreement and detailed information on both TIS's user-controlled approach to key recovery and IBM's SecureWay Key Management Framework can be found on the World Wide Web at www.tis.com or at www.ibm.com/security.

###

About Trusted Information Systems

Trusted Information Systems, Inc., is a leading provider of comprehensive security solutions for protection of computer networks, including global Internet-based systems, internal networks, and individual workstations and laptops. The Company develops, markets, licenses, and supports the Gauntlet® family of firewall products and other network security products as well as TIS's patented RecoverKey ™ technology, which is the first and only key recovery system to meet US government requirements for export. In addition to providing leading edge information security products, TIS performs an array of services in the areas of cryptography, security consulting, training, and advanced research and engineering for commercial and government customers.

About IBM SecureWay

The SecureWay Key Management Framework is part of the broad IBM SecureWay portfolio of security hardware and software products, solutions, services, consulting, and research activities. The SecureWay family provides end-to-end security solutions such as cryptographic facilities, single-sign-on, distributed security administration, access control, firewalls, secure web servers and browsers, secure electronic commerce, smart cards, anti-virus and overall Internet security. For additional information, visit the IBM SecureWay home page at http://www.ibm.com/security

About RecoverKey

TIS's patented key recovery system, RecoverKey, is unique in that it avoids the main concern typically associated with the concept of key recovery -- the handing over of encryption keys or encrypted files for storage by a third party. With RecoverKey, no keys are ever transferred to a third party unless an authorized user needs to utilize the key recovery feature. To recover the lost encryption key for a locked and lost message, a Key Recovery Center receives and decodes only a "key recovery field." The KRF holds the key that can decrypt the lost message itself but that is the only user message or encryption key data the KRC ever sees, and then only if key recovery is requested. TIS licenses its RecoverKey technology available as a software Toolkit, in Key Recovery Centers, and in the RecoverKey and RecoverKey International CSPs, which work under the Microsoft CryptoAPI.

TRUSTED INFORMATION SYSTEMS, INC.

Building a World of Trust℠

TIS BACKGROUNDER

Information on computer systems and networks is critical to the success of business and government organizations today. These organizations depend on information system security to ensure the accuracy, availability, and privacy of their information. Trusted Information Systems, Inc. (TIS) is a leading supplier of electronic security products, services, and solutions.

TIS was founded in 1983 to provide computer consulting to industry and government organizations. Today, TIS employs over 250 people in several countries, and is recognized worldwide as a pioneer in the field of computer and network security. Our mission is to be the world's premier supplier of electronic information security products, services, and solutions that enable the safe exchange of global information. Through a combination of practical and affordable solutions, system security analysis, advanced research and engineering, and training, TIS is transforming the Internet into a safe place to do business.

We have developed and customized computer and network security products and procedures to meet the needs of a variety of computing environments. To meet the high commercial demand for security over the Internet, we developed the Gauntlet family of firewall products, as well as the patented RecoverKey system for encryption key recovery. Together, the Gauntlet Internet Firewall and RecoverKey technology provide the tools to create Global Virtual Private Networks (GVPNs). This technology allows organizations to exploit the low-cost and globally accessible Internet as a transport medium, without the security risks usually associated with placing mission-critical data on the world's most public network.

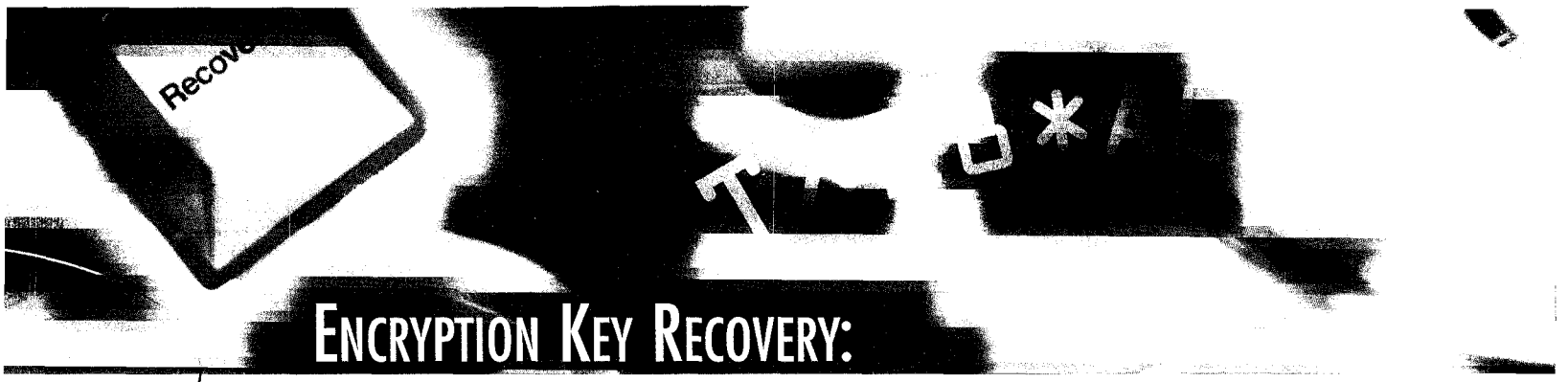
In addition to marketing and supporting commercial products, TIS is an acknowledged industry leader in advanced research and engineering of computer and communications security technology. Working under the U.S. Defense Advanced Research Products Agency (DARPA) and National Laboratory sponsorship, TIS is conducting innovative research and product development in areas such as high assurance operating systems, high assurance firewalls, world wide web servers and file servers, and techniques to improve the security of Internet infrastructure.

TIS also offers a full range of consulting services in information security policies and planning. Our clients maintain a worldwide presence in the financial, banking, telecommunications, high-tech, pharmaceutical, health care, petrochemical, utility, trade and transportation, retail, defense and government communities.

Trusted Information Systems is a public company which trades on Nasdaq under the symbol TISX. For more information on Trusted Information Systems or to arrange an interview, please call Fred Avolio at (301) 947-7101, or email avolio@tis.com.

3060 Washington Road (Rt. 97), Glenwood, Maryland 21738

(301) 854-6889 • www.tis.com • (301) 854-5363 (F)



ENCRYPTION KEY RECOVERY: RECOVERKEY™ IS THE ANSWER

Producers want exportability. Users want privacy. Government wants controls. After years of debate over the use of strong encryption, there is finally agreement: Key recovery is the answer that will allow everyone to move forward. With RecoverKey, Trusted Information Systems (TIS) has developed the first and only system that puts business needs first. Producers gain exportability by embedding RecoverKey in their products. Users can employ encryption of any strength without having to give up their keys. Businesses have an emergency spare key for vital corporate information. And here's the best part: TIS' patented RecoverKey is available and exportable today.

Trusted Information Systems' RecoverKey provides flexible, scalable, user-controlled key recovery. It will work with any key management or public key infrastructure, and can be used with any algorithm or key length. It is a technology proven to ease export of encryption products and has already been implemented by multinational organizations for their global networks. Most importantly, it's designed with the needs of business in mind.

User Controlled Key Recovery

Since a message locked up with strong encryption is completely undecipherable without a key, having a "spare key" handy for emergency file recovery makes perfect sense. But the spare key must in no way compromise security and privacy — else, why bother to encrypt in the first place? RecoverKey offers key recovery that's user-controlled.

❶ **Your key stays with your data, not with a third party.** With the RecoverKey system the emergency spare key that will unlock a particular document or file stays with the encrypted file, as a separately encrypted "Key Recovery Field."

❷ **No one stores your keys or your files.** For emergency recovery, a predesignated private sector "Key Recovery Center" can decrypt the key recovery field, using its own private key. It receives and decrypts only the key recovery field — not the file. It does so only for an authorized and authenticated requestor. It returns only the decrypted key, so the requestor can use it to decrypt the file.

❸ **Which Key Recovery Center? User's choice.** A Key Recovery Center is a security partner. Depending on your needs, you can choose a center that will allow international operations, or one that supports only domestic operations. Some companies have chosen to run their own privately held Key Recovery Centers, based in the U.S. or in Europe.

Ready Now to Allow Export of Strong Encryption

In addition to being a smart business policy, key recovery is also a prerequisite for U.S. exportability. If a U.S. firm wishes to freely export products with 56-bit encryption, it may do so during 1997 and 1998, but it must prove it has a plan for key recovery in development. If a firm wishes to export products with stronger encryption, at any time, it must have a key recovery system in place.

TIS has developed RecoverKey-International™ to enable easy export of powerful encryption products. It's the same RecoverKey system, but with export compliance built-in. While RecoverKey offers the generation of an encrypted backup key (in a key recovery field) during encryption as an option, the export-enabling International version creates a key recovery field every time, and limits the choice of Key Recovery Centers to those that have formally agreed to abide by applicable laws and regulations.

The RecoverKey Family

TIS is making its RecoverKey technology available in a variety of ways:

❶ **RecoverKey Toolkit.** TIS provides the source code to allow developers to incorporate RecoverKey's key recovery functionality into their applications. The toolkit enables product developers to choose to implement features of RecoverKey, RecoverKey-International, or both, in their products.

❷ **RecoverKey Key Recovery Center (KRC).** TIS provides the turnkey system that will allow firms to own and operate RecoverKey Key Recovery Centers. TIS will assist firms seeking "government approved" export status for Key Recovery Centers to be used with exportable products.

❸ **RecoverKey Cryptographic Service Provider (CSP).** RecoverKey is seamlessly incorporated into a TIS "crypto engine" which incorporates several popular algorithms (e.g. DES, Triple DES and 128-bit RC2/RC4) to provide encryption/decryption services with optional key recovery to a variety of CSP-compatible applications. The CSP is designed to run under the Microsoft Cryptographic API, and operates in Windows® 95 and Windows NT® environments.

❹ **RecoverKey-International CSP.** Identical to the RecoverKey CSP, except generation and verification of key recovery fields are mandatory for encryption/decryption services when key size is over 56 bits.

TIS – Industry Leader in Key Recovery

Trusted Information Systems (NASDAQ:TISX) has been providing information security solutions for more than a decade, and has been refining RecoverKey since 1994. A founding member of the computer industry alliance that is working to set global key recovery standards, TIS is firmly committed to ensuring RecoverKey's interoperability with any standards the industry develops, and will release updates of its technology as expediently as possible to serve its customers' needs. To find out more about licensing RecoverKey or about our key recovery consultation services, contact Bill Thompson by phone at (512) 263-3110, by fax (512) 669-7069, or by email thompson@tis.com. In Europe, contact Alan Liddle by phone at +44 (0) 118 930 4413, by fax +44 (0) 118 930 4412 or by email deeps@tis.com.

RECOVERKEY™

Trusted Information Systems
Building A World of Trust℠

Glenwood, MD
T (301) 854-6889
F (301) 854-5363

San Francisco, CA
T (415) 962-8885
F (415) 962-9330

Europe
T +44 (0) 118 930 4413
F +44 (0) 118 930 4412

World Wide Web
http://www.tis.com

tis

EXPORTABLE STRONG ENCRYPTION: RECOVERKEY™ CSPS

Effective use of strong encryption for global communications requires a robust cryptographic service provider (CSP). The CSP should do more than simply scramble and unscramble messages. It should work efficiently across applications, employ the strongest algorithms generally available, and run on the most popular business platform available. And it should support key recovery.

nter the CSPs that do it all: the RecoverKey™ CSP and RecoverKey-International™ CSP, from TIS. Whether you want to use strong encryption for domestic communications or over a worldwide network, TIS can ensure that you achieve the privacy, centralized key control and worldwide deployability you need.

What is a CSP?

A cryptographic service provider, whether hardware or software, manages all of the cryptographic processing that's required to generate and store encryption keys, encrypt and decrypt messages or files, perform hash functions to verify integrity, and create and verify digital signatures. The features of the CSP determine the type of encryption, as well as the key lengths that are used.

U.S. export regulations require that products offering encryption using keys over 56 bits in length incorporate a government-approved mechanism for recovery of encryption keys.

Privacy That's Virtually Impenetrable — and RecoverKey Protection

Although CSPs for domestic use are not required to have a key recovery system, corporations and users are demanding it. The reason: backup protection. Once a message or file has been encrypted using an algorithm such as 128-bit RC2/RC4 or Triple DES, it's virtually unreadable — unless you have the necessary key. If the key is lost, the information is unrecoverable.

The RecoverKey CSP generates a backup key as part of the encryption process, and separately encrypts it as a "key recovery field." In an emergency a user-designated key recovery center can unlock the key recovery field, allowing recovery of the key.

Two Key Recovery Options

The RecoverKey CSP. Key recovery is optional, and any key recovery center may be specified. This version of the CSP is available only in the U.S. and Canada. For communication between two RecoverKey CSPs in North America, users may choose whether or not they wish to enable the key recovery function. When communicating with a CSP in another country (an exported RecoverKey-International CSP) the CSP will sense the need to generate key recovery fields for international use.

The RecoverKey-International CSP. A key recovery field will be generated automatically, and only a government-approved key recovery center may be specified for that key recovery field. The CSP can function only when all required conditions are met, and will cease to function if there is an attempt to tamper with it. In other words, users at both ends must agree to accept the conditions associated with the countries where the products are resident in order for messages to be exchanged.

How the RecoverKey CSPs Work

The RecoverKey CSPs work with the widely distributed Microsoft Cryptographic Application Program Interface, or CryptoAPI, a centralized resource for all applications running on the Windows® 95 and Windows NT® operating systems.

Features*

Provider Type	PROV_RSA_FULL
Key Exchange Algorithm	PKCS#1- compliant RSA Key Exchange with modulus sizes up to 1024 bits
Signature Algorithm	PKCS#1- compliant RSA Signature/Verification with modulus sizes up to 1024 bits
Symmetric Algorithms	RC2 (up to 128 bit keys) RC4 (up to 128 bit keys) Data Encryption Standard (FIPS 46-2 DES) Triple DES
Hashing Algorithms	MD5 SHA-1
Cryptographic Engine	RSA's BSAFE
Additional Capabilities	Generation of key recovery fields for emergency access

* Included in both RecoverKey and RecoverKey-International CSPs.

The major distinction between the RecoverKey and RecoverKey-International CSPs, in CryptoAPI terms, is that the RecoverKey-International CSP always generates and verifies that the appropriate key recovery field is attached to the key exchange simple key blob. With the RecoverKey CSP, generation of the key recovery field is optional, at the user's choice, except when communicating with an export-version CSP.

Users who wish to generate additional key recovery fields (for an on-site as well as an off-site key recovery center, for example), can do so with both the RecoverKey and RecoverKey-International CSPs.

To Find Out More, Call TIS

Trusted Information Systems (NASDAQ:TISX) has been providing information security solutions for more than a decade, and has been refining RecoverKey since 1994. A founding member of the computer industry alliance that is working to set global key recovery standards, TIS is firmly committed to ensuring the RecoverKey CSP's interoperability with any standards the industry develops, and will release updates of its technology as expediently as possible to serve its customers' needs. To find out more about RecoverKey CSPs, contact Bill Thompson by phone at (512) 263-3110, by fax (512) 669-7069, or by email thompson@tis.com. In Europe, contact Alan Liddle by phone at +44 (0) 118 930 4413, by fax +44 (0) 118 930 4412 or by email deeps@tis.com.

RECOVERKEY™

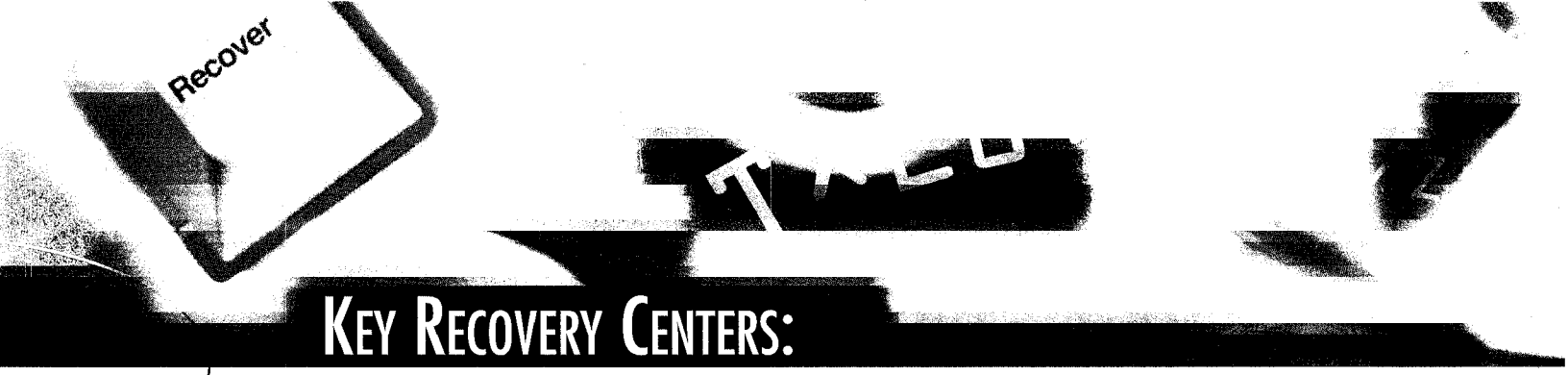
Trusted Information Systems
Building A World of Trust™

Glenwood, MD
T (301) 854-6889
F (301) 854-5363

San Francisco, CA
T (415) 962-8885
F (415) 962-9330

Europe
T +44 (0) 118 930 4413
F +44 (0) 118 930 4412

World Wide Web
http://www.tis.com



KEY RECOVERY CENTERS:
KEY TO UNLOCKING KEY RECOVERY

Key recovery centers operated by private-sector firms serve a vital security function in the Trusted Information Systems (TIS) approach to key recovery. They independently verify that requests for key recovery are legal and valid. And they fulfill those requests — receiving, decrypting and returning the key that will unlock a given file — without ever dealing with the file itself. These centers, several of which are already operating in the U.S. and Europe, can take many forms. They can be privately held, supporting an organization's own networks, or publicly accessible, offering key recovery as a service to customers.

The Key Recovery Center is at the heart of TIS' patented RecoverKey™ system. Yet its role is surprisingly simple and straightforward. It doesn't have access to users' data files. It doesn't store secret keys. It doesn't require users to turn over their keys in order to unlock their data. It doesn't decrypt users' files.

What it does is make a public encryption key available to a user, which the RecoverKey technology uses to create a "key recovery field" for the user's file. Then, when there's a request for recovery, the Center runs a pre-established authentication procedure, decrypts the key recovery field sent by the requestor using a private decryption key known only to the Center, and returns the secret session key to the requestor. The requestor is then able to use this key to recover his or her file.

TIS provides a Key Recovery Center as a turnkey solution, including all necessary hardware and software.

How the System Works

Encryption and decryption of the user's key recovery field is accomplished using very strong "public key" technology. This is a form of encryption in which two keys are required: a "public" key that can be published and used by others to encrypt their data, and a paired "private" key that is used for decryption, and never revealed to anyone.

Types of Key Recovery Operations

❶ **Optional or mandatory key recovery capability.** Organizations want key recovery for different reasons. Some want it as an optional feature. Companies seeking to meet U.S. government requirements for general export of strong encryption will need to enable key recovery functionality for all encryption sessions.

The User*	The Key Recovery Center (KRC)
❶ Purchases a RecoverKey-enabled encryption product.	❶ Purchases a Key Recovery Center system from TIS.
❷ Registers with a chosen KRC, and provides identifying information for future authentication.	❷ Registers users and issues an identifier called an Access Rule Index (ARI) for each registration; issues certificates that provide the Center's public key; maintains a secure database of users and their identifying information.
❸ Creates encrypted files which include a key recovery field (a "spare key" for the session, and an ARI, encrypted using the KRC's public key).	—
❹ When recovery is necessary, obtains a copy of the key recovery field and sends it to the KRC, along with authentication information.	❹ Uses its private key to decrypt the key recovery field and obtain the ARI; authenticates the requesting user; returns the session key to the user.
❺ Uses the session key to decrypt the original file.	—

* Any organization has many encryption users. Here the user is assumed to be the person selected to have recovery privileges.

❷ Privately held or publicly available key recovery centers. Some companies may want to operate their own KRCs "in-house." Such operations can meet the companies' internal needs and may be able to satisfy U.S. encryption export requirements. Other companies will seek out Key Recovery Centers operated on a for fee basis by financial institutions, authentication service providers or other organizations.

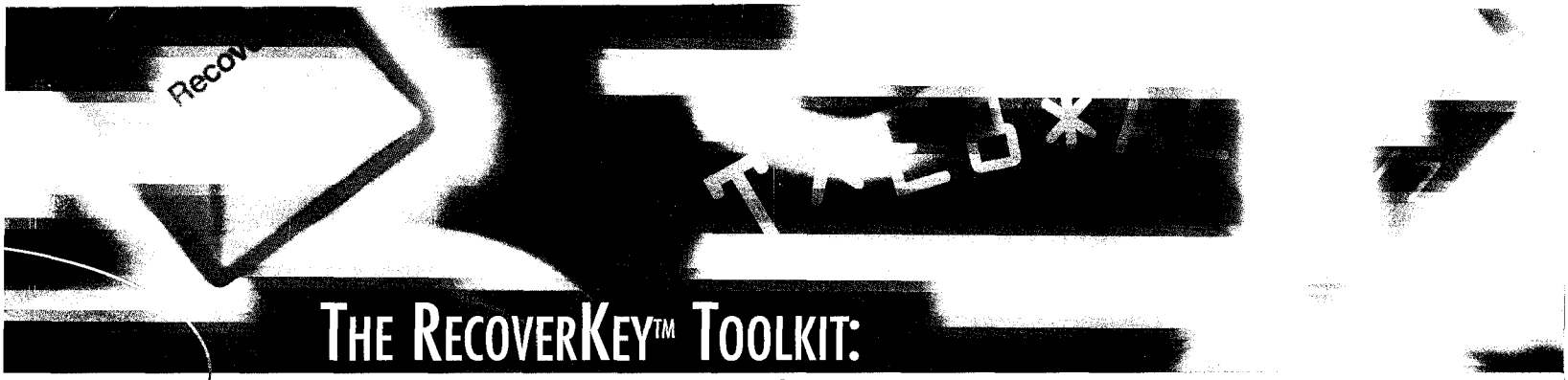
❸ "Government-approved" status. The RecoverKey system can operate with any public key infrastructure or key management system. However, the system may need to be specially configured to meet various government requirements. U.S. export regulations, for example, require that products with strong encryption include mandatory key recovery with limited interoperability. RecoverKey-International™ allows products to meet this requirement. U.S. export regulations also mandate use of only approved Key Recovery Centers. Other countries may have other requirements — or none at all.

To Find Out More, Call TIS

Trusted Information Systems (NASDAQ:TISX) has been providing information security solutions for more than a decade, and has been refining RecoverKey since 1994. A founding member of the computer industry alliance that is working to set global key recovery standards, TIS is firmly committed to ensuring RecoverKey's interoperability with any standards the industry develops, and will release updates of its technology as expediently as possible to serve its customers' needs. To find out more about licensing RecoverKey or about our key recovery consultation services, contact Bill Thompson by phone at (512) 263-3110, by fax (512) 669-7069, or by email thompson@tis.com. In Europe, contact Alan Liddle by phone at +44 (0) 118 930 4413, by fax +44 (0) 118 930 4412 or by email deeps@tis.com.

RECOVERKEY™
Trusted Information Systems
Building A World of Trust™
Glenwood, MD
T (301) 854-6889
F (301) 854-5363
San Francisco, CA
T (415) 962-8885
F (415) 962-9330
Europe
T +44 (0) 118 930 4413
F +44 (0) 118 930 4412
World Wide Web
http://www.tis.com
tis

GENUINE RSA ENCRYPTION ENGINE



THE RECOVERKEY™ TOOLKIT: YOUR KEY TO GLOBAL BUSINESS

Your cryptographic products deserve a global market.

But to export strong encryption you need key recovery. You don't want to sacrifice user privacy or their control over their keys. And you're not about to go through a major redesign. Enter RecoverKey. It can be embedded transparently in any cryptographic application, allowing it to become exportable. And it provides flexible, scalable user-controlled key recovery — today.

Trusted Information Systems' (TIS) patented RecoverKey technology lets companies meet government requirements for general export of strong encryption. And — unlike other approaches to key recovery — control of encryption keys and of key management stays in users' hands. The RecoverKey toolkit provides all the interfaces, libraries, utilities and sample code that developers need to add key recovery to their software and hardware products. Simple in concept, RecoverKey is highly flexible in implementation. It is algorithm-independent, works with any length key, and can work in any public key or key management infrastructure.

Flexibility

The toolkit code can be embedded in either communications or storage applications, and can reside in anything from firmware (a smart card or PC card) to high-level Windows® modules. The toolkit works equally well with many popular algorithms, including 128-bit RC2, 128-bit RC4, DES and Triple DES.

Scalability

The toolkit has been designed so that a single recovery application provides the recovery capability for many different types of crypto applications. Because there is never any central database of users' keys or of users' encrypted files, the user base for key recovery can be of unlimited size.

User Control

The toolkit allows a crypto engine to generate a "key recovery field" for a message or file as an integral part of the encryption process. The hidden "spare key" stays with the data, in its key recovery field, securely locked up with a public key belonging to a user-selected key recovery center. Users maintain control of their keys and their files. If recovery is needed, the key recovery center deals only with the key recovery field, not with the data.

Exportability

The toolkit may be used to enable exportability. While the basic RecoverKey application offers the creation of an encrypted backup key (in a key recovery field) during encryption as an option, the export-approved International version creates a key recovery field every time, and limits the choice of key recovery centers to those that have formally agreed to abide by applicable laws and regulations.

What's In the Toolkit

The toolkit contains the written protocol and design specifications, as well as the C code, for RecoverKey and/or RecoverKey-International™ implementation.

1. **The Registration module** gives users the ability to register with a key recovery center (KRC) of their choice. It contains all the code needed to:
   - Communicate with the KRC securely
   - Retrieve the current KRC public key certificate
   - Choose an authentication method for recovery
   - Register with the KRC and store authentication data securely.

2. **The Application module** is embedded within the cryptographic engine used to generate and exchange keys and encrypt or decrypt data. (This can be a custom application, a software cryptographic service provider (CSP), or a hardware token.) This module creates an encrypted spare session key as an integral part of the encryption function. It contains a TIS public root key for the key recovery center certification hierarchy, and all code needed to:
   - Create a valid key recovery field
   - Create a valid recovery verification field
   - Verify a key recovery field (receiver checking)
   - Validate a key recovery center certificate.

3. **The Recovery module** communicates with the key recovery center to decrypt the key recovery field and recover the session key. It contains the code needed to:
   - Determine the key recovery center's identity
   - Send the key recovery field securely to the key recovery center
   - Respond to the authentication mechanisms specified by the KRC
   - Receive the session key from the key recovery center securely.

The RecoverKey toolkit can be easily integrated into any application development environment that can deal with the portable C language. Each module is written as a stand-alone routine, and can be embedded independently of the other parts of the toolkit if desired. All access and interface routines are layered to allow you to use as much or as little of the toolkit as you need. Operating system interfaces are minimized and modularized to ensure that the toolkit functions can be easily ported to any operating environment.

To Find Out More, Call TIS

Trusted Information Systems (NASDAQ:TISX) has been providing information security solutions for more than a decade, and has been refining RecoverKey since 1994. A founding member of the computer industry alliance that is working to set global key recovery standards, TIS is firmly committed to ensuring RecoverKey's interoperability with any standards the industry develops, and will release updates of its technology as expediently as possible to serve its customers' needs. To find out more about licensing RecoverKey or about our key recovery consultation services, contact Bill Thompson by phone at (512) 263-3110, by fax (512) 669-7069, or by email thompson@tis.com. In Europe, contact Alan Liddle by phone at +44 (0) 118 930 4413, by fax +44 (0) 118 930 4412 or by email deeps@tis.com.

RECOVERKEY™

Trusted Information Systems
Building A World of Trust™

Glenwood, MD
T (301) 854-6889
F (301) 854-5363

San Francisco, CA
T (415) 962-8885
F (415) 962-9330

Europe
T +44 (0) 118 930 4413
F +44 (0) 118 930 4412

World Wide Web
http://www.tis.com